CNS 12/2013

Dictamen en relació amb la consulta formulada per una organització sobre la interpretació de l'article 104 RLOPD i si els sistemes de xifratge que empren l'algoritme de xifratge simètric AES-128 o AES-256 es troben en compliment del marc legal vigent

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit en el que es demana que l'Autoritat emeti un dictamen per valorar si els sistemes de xifratge que empren l'algoritme de xifratge simètric AES-128 o AES-256 es troben en compliment del marc legal vigent.

En concret, exposa que, atès que l'article 104 del RLOPD preveu que quan es transmetin dades de caràcter personal de nivell alt a través de xarxes públiques o xarxes sense fil s'ha de fer xifrant les dades o utilitzant qualsevol altre mecanisme que garanteixi que la informació no sigui intel.ligible ni manipulada per tercers, es plantegen dubtes sobre quins sistemes de xifratge ofereixen suficients garanties.

Analitzada la consulta, que s'acompanya de l'Informe 494/2009 de l'Agencia Española de Protección de Datos, i vistos els informes del coordinador d'Auditoria i Seguretat de l'Autoritat i de l'Assessoria Jurídica emeto el següent dictamen:

I

(...)

II

Es consulta en primer lloc quina interpretació fa l'APDCAT de l'article 104 del Reglament de desplegament e la Llei orgànica de protecció de dades (RLOPD), aprovat pel R. Decret 1720/2007, de 21 de desembre.

L'article 104 del RLOPD estableix el següent:

> "Quan conforme a l'article 81.3 s'hagin d'implantar les mesures de seguretat de nivell alt, la transmissió de dades de caràcter personal a través de xarxes públiques o xarxes sense fil de comunicacions electròniques s'ha de fer xifrant les dades esmentades o bé utilitzant qualsevol altre mecanisme que garanteixi que la informació no sigui intel•ligible ni manipulada per tercers."

Les dades a què es refereix l'article 81.3 RLOPD, al qual es remet l'article 104de la mateixa norma, són aquelles que requereixen nivell alt de seguretat, o sigui:

a) Els que es refereixin a dades d'ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual.

b) Els que continguin o es refereixin a dades obtingudes per a fins policials sense consentiment de les persones afectades.
c) Els que continguin dades derivades d'actes de violència de gènere.

En aquests supòsits, d'acord amb l'article esmentat, s'ha de garantir la confidencialitat i la integritat de les dades personals durant el seu transport pels canals de comunicació esmentats en aquest article del RLOPD (xarxes públiques o xarxes sense fil de comunicacions electròniques).

L'ús de la criptografia és en l'actualitat la manera més eficaç i eficient d'aconseguir la confidencialitat i la integritat de les dades en la seva transmissió, sempre que es tingui en compte que hi ha diverses alternatives a l'hora d'utilitzar-la i que segons l'escenari que es vulgui protegir, l'ús d'una o altra alternativa poden oferir o no suficients garanties per a l'adequada protecció de les dades trameses.

De fet, l'article 104 RLOPD permet garantir la seguretat, be sigui xifrant les dades esmentades, be sigui utilitzant "*qualsevol altre mecanisme que garanteixi que la informació no sigui intel•ligible ni manipulada per tercers*." I això permet que la criptografia pugui utilitzar-se a diferents nivells: es pot utilitzar per xifrar el canal de comunicació o bé per xifrar les dades a transmetre.

Si bé el xifratge el canal de comunicació pot facilitar aquesta tasca, això no sempre serà possible perquè en aquest procés poden intervenir aspectes no sotmesos al control de qui transmet les dades. Per exemple, si es vol enviar un correu electrònic a un destinatari que utilitza un servidor de correu diferent, podrem xifrar el canal de comunicació entre el nostre ordinador i el nostre servidor de correu, però això no evitaria que la transmissió del missatge des del nostre servidor de correu fins al servidor de correu del destinatari estigués desprotegida, ni tampoc protegiria la transmissió des del servidor de correu del destinatari fins al seu ordinador.
En tots els casos en què no es pugui xifrar el canal de comunicació des de l'origen fins el destí o fins a un punt a partir del qual la informació no passi per xarxes públiques o sense fil per arribar al destí, caldrà xifrar les dades que es vulgui transmetre.

III

En segon lloc, la consulta planteja si els sistemes de xifratge que empren els algoritmes de xifratge simètric AES-128 i AES-256 compleixen el marc legal vigent que es deriva de l'article 104 RLOPD esmentat. Per tant, cal analitzar quin tipus de criptografia cal utilitzar per tal de donar compliment al que estableix l'article 104 RLOPD.

Amb caràcter previ però, i per exposar millor les diferències entre els diversos tipus de criptografia, cal exposar, encara que sigui breument, com funcionen els sistemes de xifratge.

Els sistemes de xifratge consten de dos processos:

- Xifratge: En aquest procés es transformen les dades (text en clar) en unes dades illegibles (text xifrat) mitjançant l'aplicació de una funció matemàtica complexa (algoritme de xifratge) i una clau de xifratge.

- Desxifratge: En aquest procés es transforma el text xifrat en el text en clar mitjançant una segona funció matemàtica complexa i una clau de desxifratge.

Depenent de si les claus de xifratge i desxifratge son iguals o no, podem parlar de:

Criptografia simètrica o de clau privada: en aquest tipus de criptografia s'utilitza la mateixa clau per xifrar i desxifrar la informació.

Criptografia asimètrica o de clau pública: en aquest tipus de criptografia s'utilitza una clau per xifrar la informació (anomenada clau pública) i una altra clau per desxifrar-la (anomenada clau privada). La clau pública es pot divulgar públicament sense posar en perill la confidencialitat de les dades.

Hi ha altres tipus de criptografia, però són variants o combinacions dels tipus de criptografia que hem descrit.

La criptografia simètrica és habitualment més ràpida d'utilitzar que el de clau pública, però té el problema que el remitent i el destinatari de la informació s'han de transmetre la clau de xifratge de forma segura. La criptografia simètrica s'utilitza per xifrar grans volums d'informació. Alguns algoritmes que utilitzen criptografia simètrica són DES, 3DES, Blowfish, IDEA, RC2, RC4, RC5 i AES.

La criptografia de clau pública resol el problema de distribució de les claus de xifratge, però té el problema que és lenta. Alguns algoritmes basats en criptografia de clau pública són Diffie-Hellman, RSA, ElGamal, DSS i Merkle- Hellman.

Els factors que determinaran quin tipus de criptografia convé utilitzar són:

-El volum de la informació a xifrar
-La gestió de les claus de xifratge i desxifratge

Per exemple, si s'han de transmetre grans volums d'informació xifrada entre un grup reduït de persones, la utilització de la criptografia simètrica seria a priori la millor alternativa, però si el mateix volum d'informació s'hagués de transmetre entre un alt nombre de persones, caldria valorar si es pot assumir la dificultat de gestionar i distribuir les claus de desxifratge entre un gran nombre de destinataris.

En aquest últim cas podria més fàcil optar per sistemes de xifratge de clau pública per la facilitat de distribuir les claus de xifratge, encara que haguem de patir lentitud en el xifratge de les dades.

Per últim, un altre factor a tenir en compte a l'hora d'escollir el sistema de xifratge és la fortalesa criptogràfica. La fortalesa criptogràfica és la capacitat del sistema de xifratge de protegir la informació davant d'un atac. Aquesta fortalesa pot dependre de molts factors, però els dos principals són la capacitat que tingui l'atacant d'invertir l'algoritme de xifrat sense conèixer la clau i la dificultat que tingui l'atacant de descobrir la clau de desxifrat. Com més llarga sigui la clau de desxifrat més difícil serà descobrir-la.

A l'hora d'escollir un sistema de xifratge convé assegurar-se que aquest no contingui vulnerabilitats conegudes, ja sigui perquè s'hagi demostrat que l'algoritme utilitzat no és segur o perquè el temps per calcular totes les claus possibles per desxifrar les dades pugui permetre a un atacant desxifrar les dades sense esforços desproporcionats. Per exemple, si s'estima que el temps per calcular totes les claus d'un sistema de xifratge és de mil anys, i s'utilitza per xifrar un informe d'un pacient, podríem dir que el sistema és prou segur, ja que el temps que legalment hem de protegir la informació del pacient és inferior al temps que un suposat atacant hauria de dedicar per desxifrar la informació.

De totes maneres, les mesures de seguretat s'han d'adoptar sempre tenint en compte l'estat de les tecnologies i els riscos als quals estan exposades les dades. Un sistema de xifratge pot ser considerat segur en un determinat moment i deixar de ser-ho un temps després perquè s'ha descobert una vulnerabilitat o perquè amb l'increment de la potencia dels ordinadors el temps de càlcul de les claus de desxifratge s'ha reduït ostensiblement.

Tal com dèiem al principi, l'article 104 del RLOPD obliga a garantir la confidencialitat i la integritat de les dades personals de nivell alt durant el seu transport a través de xarxes públiques o xarxes sense fil de comunicacions electròniques. Dit d'altra manera, la necessitat de transmetre aquestes dades utilitzant canals de comunicació públics o fàcilment interceptables no ha d'afectar l'obligació de protegir aquest tipus de dades personals de la manipulació o de l'accés o tractament no autoritzats.

Des de el nostre punt de vista, per a que els sistemes de xifratge que empren els algoritmes de xifratge simètric AES-128 i AES-256 complissin el marc legal vigent s'hauria de verificar:

- Que l'algoritme del sistema de xifratge escollit no tingués vulnerabilitats conegudes susceptibles de ser explotades.

- Que el sistema o eina de xifratge no tingués vulnerabilitats conegudes susceptibles de ser explotades.

- Que la gestió i distribució de les claus de xifratge/desxifratge sigui adequada.

Pel que fa a la primera qüestió, això és que l'algoritme del sistema de xifratge escollit no tingués vulnerabilitats conegudes susceptibles de ser explotades, el mes de juny de 2003, el Govern dels Estats Units d'Amèrica va anunciar que l'algoritme de xifratge simètric Advanced Encryption Standard (AES) podia ser utilitzat per xifrar informació classificada del propi Govern. Amb posterioritat a aquesta data s'han anunciat possibles atacs teòrics que podrien trencar l'algoritme, però la gran majoria d'experts criptogràfics no han trobat vulnerabilitats reals que en la pràctica posin en dubte la fortalesa d'aquest algoritme en l'actualitat. Per això, no sembla que a data d'avui hi hagi prou elements per posar en dubte la fortalesa de l'algoritme de xifratge AES (en les seves variants de 128 bits i 256 bits).

Ara bé, tal com exposàvem més amunt, la seguretat del xifratge no depèn només de l'algoritme del sistema de xifratge escollit, sinó també del sistema o eina de xifratge i de que la gestió i distribució de les claus de xifratge/desxifratge sigui adequada. Per això, per a poder fer una anàlisi completa de la consulta efectuada caldria tenir en compte també quina eina o sistema de

xifratge es vol utilitzar per xifrar la informació a transmetre i de quina manera es gestionaran i distribuiran les claus necessàries per xifrar i desxifrar aquesta informació.

IV

Pel que fa a al sistema o eina de xifratge, en la consulta es fa referència als mecanismes de xifratge a través d'Adobe Acrobat (fitxers pdf) i del xifratge a través de Winzip. A aquests efectes, s'adjunta un informe de l'Agència Espanyola de Protecció de Dades de l'any 2009 (Informe 0494/2009) on es conclou que el sistema de xifratge d'ambdós sistemes resultava vulnerable. L'anàlisi d'aquesta qüestió requereix distingir entre un i altre sistema. Ara bé, hem d'avançar que, sens perjudici que les conclusions obtingudes en aquell informe poguessin resultar plenament adequades, l'anàlisi que es durà a terme en el present dictamen no es refereix a les versions dels programes que van ser analitzats en aquell informe per l'AEPD sinó a les darreres versions disponibles, a data d'avui, de cadascun d'aquests programes. Tal com hem exposat més amunt, la vulnerabilitat dels sistemes és una qüestió que pot anar canviant en el temps.

Pel que fa a l'Adobe Acrobat, el seu darrer producte és l'Adobe Acrobat XI, disponible des de finals del 2012. Aquest producte no és una millora de l'anterior versió (Adobe Acrobat X) sinó que es un producte nou. Quant a les característiques tècniques referents a les tècniques de xifratge que ofereix aquest producte, cal indicar que el xifratge es realitza amb 256-bit AES i permet el xifratge de tots els continguts, inclosos metadades o documentació adjunta.

A nivell de seguretat del propi producte, des de la seva aparició s'han publicat diferents vulnerabilitats de seguretat que han estat: CVE-2012-1530, CVE-2013-0601, CVE-2013-0602, CVE-2013-0603, CVE-2013-0604, CVE-2013-0605, CVE-2013-0606, CVE-2013-0607, CVE-2013-0608, CVE-2013-0609, CVE-2013-0610, CVE-2013-0611, CVE-2013-0612, CVE-2013-0613, CVE-2013-0614, CVE-2013-0615, CVE-2013-0616, CVE-2013-0617, CVE-2013-0618, CVE-2013-0619, CVE-2013-0620, CVE-2013-0621, CVE-2013-0622, CVE-2013-0623, CVE-2013-0624, CVE-2013-0626, CVE-2013-0627, CVE-2013-0640 i CVE-2013-0641.

Tot aquest llitat de vulnerabilitats que ha presentat el producte han estat resoltes amb l'aplicació de les diferents actualitzacions que Adobe Acrobat ha anat publicant, per la qual cosa, en l'actualitat, no existeixen vulnerabilitats publicades sobre aquest producte.

Pel que fa al Winzip, la darrera versió és el Winzip 17, disponible des de finals del 2012. Aquest producte és una millora de l'anterior versió (WinZIP 16.5). Aquest producte permet el xifratge amb 128-bit AES o 256-bit AES. També permet establir polítiques de contrasenyes (qualitat de contrasenyes) per tal de millorar la seguretat en quant a l'accés dels fitxers.

Des del punt de vista de les vulnerabilitats tècniques sobre aquest producte, no existeix cap vulnerabilitat publicada.

Per tant, a partir de la informació publicada sobre els dos productes analitzats, així com de les vulnerabilitats publicades en repositoris públics de vulnerabilitats tècniques de productes, podem indicar que els dos productes no presenten, a data d'avui, vulnerabilitats tècniques sense resolució.

Cal tenir present però la publicació constant de vulnerabilitats, amb la qual cosa, el fet que en l'actualitat no siguin vulnerables no implica que en un futur no puguin ser-ho, amb la qual cosa, es recomana la instal·lació de les diferents actualitzacions que poguessin publicar els fabricants d'aquests productes

D'acord amb les consideracions fetes en aquests fonaments jurídics en relació amb la consulta plantejada en relació amb si els sistemes de xifratge que empren l'algoritme de xifratge simètric AES-128 o AES-256 es troben en compliment del marc legal vigent, es fan les següents,

Conclusions

A data d'avui l'algoritme de xifratge AES (en les seves variants de 128 bits i 256 bits), pot considerar-se que compleix els requisits de seguretat establerts per l'article 104 del RLPOD.

Les eines de xifratge Adobe Acrobat XI i Winzip 17 no presenten, a data d'avui, vulnerabilitats tècniques sense resolució.

Ara bé, a l'hora de garantir la seguretat del sistema de xifratge caldrà tenir en compte, també, de quina manera es gestionaran i distribuiran les claus necessàries per xifrar i desxifrar aquesta informació

Barcelona, 4 de març de 2013